DEFENCE **R&D** DÉFENSE

Comparison of Identify-Friend-Foe and Blue-Force Tracking Decision Support for Combat Identification

David J. Bryant
David G. Smith

Canada

Comparison of Identify-Friend-Foe and Blue-Force Tracking Decision Support for Combat Identification

David J. Bryant
David G. Smith

Defence R&D Canada – Toronto

Principal Author

Original signed by David J. Bryant

David J. Bryant

Acting Section Head, Human Systems Integration

Approved by

Original signed by Joseph V. Baranski

Joseph V. Baranski

Chief Scientist

Approved for release by

Original signed by K. C. Wulterkens

K. C. Wulterkens

For Chair, Knowledge and Information Management Committee

Abstract

Technologies to support Combat Identification (CID) are rapidly evolving and may be deployable to dismounted soldiers in the future. Two experiments examined the effectiveness of Identify-Friend-Foe (IFF) and Blue-Force Tracking (BFT) decision support for dismounted infantry soldiers. Subjects played the role of a dismounted infantry soldier in a first-person perspective environment and engaged a series of simulated targets. Subjects attempted to engage (i.e., shoot) only those figures that were enemies. Results demonstrated that subjects performed better overall when they were able to use a Decision Support System (DSS) than perform the task without assistance. There was no difference in effectiveness of the IFF and BFT systems. Adding a 10 second delay to the updating of position information in the BFT dramatically reduced the effectiveness of a BFT, regardless of whether subjects knew about the delay or not.

Résumé

Les technologies servant à appuyer l'identification au combat (IDCbt) évoluent rapidement et pourraient éventuellement être mises à la disposition de chaque soldat à pied. Deux expériences ont permis d'examiner l'efficacité des systèmes d'aide à la décision *Identification ami ou ennemi* (IAE) et *Suivi des forces bleues* (SFB) pour les fantassins à pied. Chacun des participants a joué le rôle d'un fantassin à pied dans une perspective de premier intervenant et devait engager une série de cibles simulées. Les sujets ne devaient tirer que sur les figures ennemies. Selon les résultats obtenus, les participants ont obtenu un meilleur rendement général lorsqu'ils ont eu recours à un système d'aide à la décision (SAD) que lorsqu'ils ont exécuté la tâche sans aide. Aucune différence n'a été notée quant à l'efficacité des systèmes IAE et SFB. Une période d'attente de 10 secondes appliquée à la mise à jour des données sur la position dans le système SFB a réduit sensiblement l'efficacité du SFB, sans égard au fait que les sujets étaient mis au courant du délai ou non.

This page intentionally left blank.

Executive summary

Comparison of Identify-Friend-Foe and Blue-Force Tracking Decision Support for Combat Identification

[David J. Bryant; David G. Smith]; DRDC Toronto TR 2009-214; Defence R&D Canada – Toronto.

Introduction: Combat Identification (CID) is the process by which enemies are identified and a key element of combat effectiveness. Two types of systems have been proposed as decision support for CID. Blue-Force Tracking (BFT) systems seek to mitigate the risk of fratricide by supplying positional information regarding friendly units to enhance situation awareness. Identify-Friend-Foe (IFF) systems employ transponders attached to friendly units that return a coded signal whenever they are targeted by a particular kind of transmission (e.g., infrared, radar). Soldiers with the appropriate signal generator and receiver can interrogate potential targets and identify a targeted unit as a friend.

Results: Two experiments examined the effectiveness of IFF and BFT decision support for dismounted infantry soldiers in a simulated environment. The first experiment directly compared CID performance when subjects had access to a rifle-mounted IFF or hand-held BFT system as opposed to no decision support. Twenty-four subjects performed an experimental CID task in three conditions (with no Decision Support System [DSS], with a rifle-mounted IFF, and with BFT) and their Hit (correct engagement of an enemy) and False Alarm (FA) (incorrect engagement of a friend) rates were measured. Hit rates were high in all conditions but significantly larger in the IFF and BFT than No DSS condition. In contrast, the FA rate in the No DSS condition was significantly greater than that in both the IFF and BFT conditions. Subjects were significantly more sensitive in the IFF and BFT conditions compared to the No DSS condition. Whereas subjects showed negative bias (i.e., a tendency to not engage) in the No DSS and IFF conditions, they exhibited positive bias (i.e., tendency to engage) in the BFT condition. Experiment 2 examined the impact of a 10 second delay between movement of friendly units and the updating of a hand-held BFT on subjects' CID performance. Twenty-four subjects performed four conditions, a baseline with BFT providing real-time positional information, a 10 second delay condition with no warning that the BFT data would lag actual movement, a 10 second delay condition in which subjects were told of the delay, and a final end baseline with real-time update of the BFT. Adding the delay did not significantly reduce subjects' Hit rate but did significantly increase subjects' FA rate. Subjects exhibited a strong response bias toward engaging targets in both delay conditions.

Significance: Taken together, the results of the experiments indicate the promise of personal IFF and BFT devices to drastically reduce the likelihood of fratricide by dismounted infantry soldiers on other soldiers. The results, however, also indicate that the effectiveness of these devices can be dramatically reduced when the devices do not work perfectly in real-time.

Future Plans: Given normal operational conditions that include inclement weather, dust and other environmental factors that can disrupt the functioning of IFF and BFT devices, it is crucial to further examine how the decision making of the human user of these devices will be affected by factors that reduce the effectiveness of those devices.

Sommaire

Comparaison des systèmes d'aide à la décision *Identification ami ou ennemi* et *Suivi des forces bleues* pour l'identification au combat

[David J. Bryant; David G. Smith]; DRDC Toronto TR 2009-214; Defence R&D Canada – Toronto.

Introduction : L'identification au combat (IDCbt), le processus par lequel les ennemis sont identifiés, est un élément clé de l'efficacité au combat. Deux types de systèmes ont été proposés comme aides à la décision aux fins de l'IDCbt. Les systèmes de Suivi des forces bleues (SFB) visent à atténuer les risques de fratricide en fournissant des données sur la position des unités amies permettant d'améliorer la connaissance de la situation. Les systèmes d'Identification ami ou ennemi (IAE) utilisent des transpondeurs reliés à des unités amies qui renvoient un signal codé chaque fois qu'ils sont ciblés par une transmission donnée (infrarouge, radar, etc.). Les soldats munis du générateur et récepteur de signaux approprié peuvent interroger les cibles potentielles et identifier une unité ciblée comme amie.

Résultats : Deux expériences ont permis d'examiner l'efficacité des aides à la décision IAE et SFB pour les fantassins à pied en milieu de simulation. La première expérience a permis de comparer directement l'efficacité de l'IDCbt pendant que les sujets avaient accès à un système IAE et à un fusil ou à un système SFB portable, par opposition à l'absence d'aide à la décision. Vingt-quatre sujets ont exécuté une tâche expérimentale d'IDCbt dans trois conditions (sans système d'aide à la décision [SAD], munis d'un système IAE et d'un fusil, ou munis d'un système SFB). On a évalué leur taux de succès (engagement justifié d'un ennemi) et leur taux de fausse alerte (FA) (engagement à tort d'un ami). Les taux de succès étaient élevés dans toutes les conditions, mais sensiblement meilleurs lorsque les sujets disposaient de systèmes IAE et SFB qu'en l'absence de SAD. Par contraste, le taux de fausse alerte en l'absence de SAD était de beaucoup supérieur à celui enregistré en présence des IAE et SFB. Les participants avaient une sensibilité de loin supérieure lorsqu'ils étaient munis de systèmes IAE et SFB qu'en l'absence de SAD. Alors que les sujets faisaient preuve d'un parti pris négatif (c.-à-d., une tendance à ne pas engager la cible) en l'absence de SAD et en présence d'IAE, ils ont fait montre d'un parti pris positif (c.-à-d., une tendance à engager la cible) en présence du SFB. Durant la seconde expérience, on a examiné l'impact d'une période d'attente de 10 secondes, entre le déplacement des unités amies et la mise à jour des SFB portables, sur le rendement d'IDCbt des participants. Vingt-quatre sujets ont été soumis à quatre conditions : un niveau de référence dans lequel le SFB fournissait des données de position en temps réel, un délai de 10 secondes sans que le sujet soit averti du fait que les données du SFB paraîtraient en retard par rapport aux déplacements réels, un délai de 10 secondes dont les sujets étaient informés, et un dernier niveau de référence avec mise à jour en temps réel du SFB. L'ajout de la période d'attente n'a pas réduit sensiblement le taux de succès de l'engagement des participants, mais il a augmenté le taux de fausse alerte de manière significative. Les sujets ont fait montre d'un parti pris nettement favorable à l'engagement des cibles dans les deux situations où il y avait un délai d'attente.

Portée : Globalement, les résultats des expériences laissent supposer que des dispositifs personnels d'IAE et de SFB permettraient de réduire sensiblement la probabilité de fratricide entre les fantassins à pied et d'autres militaires. Cependant, les résultats indiquent aussi que l'efficacité de ces dispositifs peut être réduite de manière significative lorsque les appareils ne fonctionnent pas parfaitement en temps réel.

Recherches futures : Étant donné que dans les conditions opérationnelles normales, les intempéries, la poussière et d'autres facteurs environnementaux peuvent nuire au fonctionnement des dispositifs d'IAE et de SFB, il est essentiel d'examiner plus en profondeur l'influence des facteurs qui réduisent l'efficacité de ces appareils sur le processus décisionnel de l'humain appelé à s'en servir.

This page intentionally left blank.

Table of contents

List of figures

List of tables

Acknowledgements

The experiment reported here was completed with the invaluable assistance of Matthew Lamb and Elaine Maceda.

This page intentionally left blank.

Introduction

Combat Identification (CID) is the capability to rapidly and accurately identify friendly, enemy and neutral forces, manage and control the battlespace, and optimally employ weapons and forces [1]. The goal of the decision maker in CID is to ensure that when a weapon is fired, it is fired at an appropriate target. Therefore, CID involves rapidly and accurately identifying the allegiance (e.g., friend, enemy, neutral) of contacts detected in the battlespace based on all available sources of data. Ultimately, the purpose of CID is to gain the maximal combat effectiveness possible, which involves minimizing losses caused by both enemy and friendly fire [2].

In most operational settings, surveillance, navigation, and networking data are available and must be considered to correctly identify targets. Thus, CID requires at least three general elements: situation awareness (SA), target identification, and tactics, techniques, and procedures (TTPs) (e.g., Dean & Handley [2]). SA refers to the perception and understanding of the operational environment needed to act effectively in that environment. CID clearly requires SA as a precursor to the classification of entities as friendly, hostile, or neutral. Target identification is the process of making that classification judgment based on the characteristics of the entity in question in relation to the TTPs that govern how one interprets objects in the operational environment. TTPs can dramatically affect what aspects of the environment are monitored and what kinds of cues will be picked up on by soldiers. One can think of SA as providing the data about objects in the environment and TTPs providing the knowledge needed to interpret that data. Target identification is thus the process by which SA and TTPs are employed [2].

Failures of CID

It is generally the failures of CID that cause the most concern both operationally and nationally. Failure of a CID system can lead to fratricide, the inappropriate engagement and potential wounding or killing of a friendly soldier or unit, neutricide[1] (identifying a neutral contact as hostile) and injury or death to oneself caused by failing to identify an enemy contact[2] (see Harris & Syms [5]).

Causing accidental death or injury is only one of the negative effects of fratricide and neutricide. Other negative effects are listed in Table 1. Some affect the combat effectiveness of one's own forces, as fratricide can lead to loss of morale as well as a reluctance to take risk and seize the initiative. Other effects are more systemic, changing the nature of command and control or causing political or legal issues. Neutricide can likewise create political and legal issues and undermine efforts to win over local civilian populations.

Estimating the frequency of fratricide has historically been a difficult task. Generally, little reliable evidence is available and the tempo of warfare works against the preservation of sites where fratricide may have occurred [6]. Estimates from the First and Second World Wars put

---

[1] Neutricide is the term used by Dean et al. [3] to describe incidents when civilians and civilian infrastructure are accidentally targeted or misidentified and deliberately targeted.

[2] Referred to as a mistake akin to 'suicide' on the battlefield by Karsh et al. [4].

the rate of fratricide between 10% and 15% [3]. Harris and Syms [5] conducted a thorough review of historical reports and documents that indicated similar rates for those conflicts but suggested higher rates for more recent conflicts. In line with this, nearly 80% of casualties suffered by the United Kingdom in Operation Granby (first Iraq war in 1991) were attributed to friendly fire [3]. The United States (US) estimated a much lower fratricide rate in that conflict but one still higher than those estimated in earlier wars.

Table 1: Negative Effects of Fratricide and Neutricide	
Source: Dean et al. (2005) [3]	Source: U.S. Congress, Office of Technology Assessment
Casualties & damage to equipment	General degradation of cohesion and morale
Wasted time, effort, and ammunition	Loss of confidence in leadership
Drop in morale and levels of trust	Increase of leader self-doubt
Drop in unit effectiveness and excessive caution	Hesitation to use supporting combat systems
Political repercussions	Over-supervision of units
Loss of "hearts and minds" of civilian population	Loss of initiative
Unnecessary risk to own forces	Loss of aggressiveness
Disruption of tempo	Disrupted operations
Strain on coalitions if casualties inflicted on allies	Needless loss of combat power
	Hesitation to conduct limited visibility operations

Several factors potentially contribute to a greater risk of fratricide in the modern battlespace. Weapons have much longer ranges than in past conflicts, meaning that targets can be engaged before it is possible to acquire positive identification [7]. This creates a dangerous situation in which forces must be concerned that a target is a potential enemy who could fire upon them but are unable to gather the data necessary for CID. The greater range of weapon systems also means that remote sensors, which may provide only partial cues to identity, must be relied on to a greater extent. Greater mobility of forces has led to operational environments in which forces are more dispersed, making it more difficult to maintain good SA [1].

In addition to the greater risk of fratricide and neutricide, the use of more precise weapons and surveillance allows fratricides and neutricides to be more easily detected [1]. Hence accidental deaths and injuries due to friendly fire that may have gone unexplained in past conflicts may now be more accurately attributed as fratricide/neutricide.

Perhaps the most significant factor working against CID in today's environment is the increasingly asymmetric nature of conflict. Canada and her coalition partners find themselves participating in high tempo, non-linear operations with enemies who eschew traditional uniforms and employ diverse equipment. The presence of civilians further complicates the environment.

What causes CID failures?

There is no single cause for incidents of fratricide and neutricide. The major risk factors that have been identified are a) the loss of SA, and b) misidentification of the target [5] [7] [8]. Each of these factors, however, is itself a confluence of more proximal factors that break down further into human, physical, and organizational factors [2].

Human factors are characteristics or traits of human beings, related to their physiology, cognitive capabilities, and development (e.g., through training), that can negatively affect CID performance. One such factor is the natural limit to information processing capacity exhibited by people [9] which makes it difficult for soldiers to maintain SA in complex environments [7]. CID is made especially difficult for soldiers in environments such as Afghanistan by the asymmetric nature of that conflict, characterized by a difficulty in knowing who one's enemy is, where they are, and how and when they will attack. Human beings are also subject to stress and emotional states that can impair performance, leading to misidentifications, lack of fire discipline, etc. Training and education can be positive factors but poor training can impair both SA and identification [2].

Physical factors include both environmental conditions and the state of equipment, especially sensors. Environmental conditions that reduce visibility or hinder the functioning of sensors are key factors in many fratricide incidents [10]. Equipment failures can also make CID more difficult and error-prone. Increasingly, operational zones feature the presence of similar or even identical equipment being used by friendly, neutral, and enemy forces and this can cause tremendous confusion in the identification process [7]. A key problem in modern warfighting is that sensor technology has dramatically increased the range at which targets can be detected, without a concomitant increase in the capability to identify targets [11].

Operational factors pertain to the unique geographical, cultural, and historic features of the operational setting, as well as the organizational structure in which soldiers function. Operating afield in unfamiliar nations often leaves soldiers with limited knowledge of the kinds of information needed to distinguish neutral from potentially hostile factions [12]. It is often the case that such knowledge is difficult and time-consuming to acquire. Constraints imposed from higher command in the form of Standard Operating Procedures (SOP) and Rules of Engagement (ROE) can further hinder the CID process. Failures of command and control (C2) and communication frequently contribute to fratricide and neutricide incidents [10]. All of these issues are exacerbated in high-tempo operations that decrease margins of error [5].

How can CID be Improved?

There are two main approaches to improving CID performance. One is to support target identification in some fashion, typically by outfitting all friendly units with some reliable indicator such as an IFF (Identify-Friend-Foe) transponder. The other approach is to support SA in some fashion. The US Armed Forces has developed concepts for decision support to both SA and target identification [8]. In the former case, the US Armed Forces has employed visual markings, radio emission intercept, and IFF systems to assist in target identification [4] [7]. In the latter case, it has considered so-called "blue-force tracking" systems that track the positions of all friendly vehicles and transmits this information. Significant work in this area has been done by the US Joint Force Command's (USJFCOM) Coalition Combat Identification (CCID) team through its Advanced Concept Technology Demonstrations

(ACTD). Although Canada is participating in efforts to develop SA and target identification decision support tools, the CF has also worked on refining TTPs to enhance CID [13]. This work includes the development of enhanced training as well as new SOPs.

Identify-Friend-Foe (IFF) Systems

Prior to the first Persian Gulf War of the early 1990s, CID had not been viewed as a system requirement for vehicles by the US and allied nations [11]. Instead, development had focused on measures to increase the survivability of vehicles and crews. During that conflict, however, fratricide was recognized as a significant risk and attempts were made to assist decision makers with target identification judgments. For example, during the first Persian Gulf War, allied vehicles were outfitted with fluorescent orange panels, which also had chevrons painted on them (in some cases in infrared reflective paint) to differentiate them from enemy vehicles [14]. This was a relatively simple way to enhance target identification but not completely successful. Dust and smoke frequently obscured the panels and rain and fog could mask infrared reflections, rendering the identifying panels ineffective [14].

Other so-called "quick fixes" were attempted during the first Persian Gulf War [11]. The Anti-Fratricide Identification Device (AFID) was deployed to prevent air-to-ground fratricide. AFID consisted of an infrared beacon using two high-powered infrared diodes fitted with a protective collar to prevent infrared energy from being detectable by enemy ground forces. A major concern with this beacon technology was that enemy forces could detect AFID emissions and use them to target coalition vehicles. Nevertheless, another infrared emitting device, nicknamed "Budd Light" after its designer Henry "Bud" Croley, did not employ a shroud and its infrared emissions could be detected by ground forces [11]. Any collar or shroud reduced the effectiveness of the beacon as a signal to air units. Like the orange panels and infrared reflective tape, these beacons proved only marginally effective.

Infrared beacons and reflective tape are non-cooperative counter-fratricide measures, which eliminates the need for shooters to carry specialized devices to interrogate targets but makes vehicles vulnerable to detection and identification by enemy forces. Other non-cooperative approaches include Electronic Support Measures (ESM) "fingerprinting" or tagging, in which platforms that emit electromagnetic signals do so at specific pre-defined frequencies so that all friendly receivers can recognize them [1].

Given the potential for non-cooperative techniques to increase threat of enemy detection and attack, allied nations began to look at adapting IFF technologies used in aircraft for use with ground vehicles. IFF for ground units was first used during the Vietnam War and further experimented with by the North Atlantic Treaty Organization (NATO) during the 1970s and early 1980s [15]. Aircraft IFF consists of a transponder attached to the aircraft that sends out a coded signal when the transponder is illuminated by a radar. If the operator of the radar possesses the appropriate code, he/she can identify the aircraft appropriately as a friend.

Among the different technologies considered for ground-based IFF are millimetre wave (mmW), infrared laser, and radio-frequency (RF) based solutions [16]. In all cases, the system requires both a transponder to be placed on all vehicles as well as an interrogator to be placed on platforms that might engage targets. A potential problem for IFF systems is their vulnerability to "spoofing" (i.e., the false generating of a friendly signal) by the enemy [1]. Encryption of signals is necessary to reduce this problem, as well as frequent changing of

security keys. Even so, an enemy could potentially exploit IFF and beacon systems as a means to do surveillance of the battlespace [1].

It has been difficult to field effective IFF for ground units due to issues of cost, size, and weight of such systems, as well as the phenomenon of ground interference caused by the cluttered ground environment [15]. The Battlefield Combat Identification System (BCIS), however, is a successful IFF system that identifies BCIS-equipped targets even under degraded environmental conditions. BCIS is a mmW question and answer CID system that can identify friendly ground combat vehicles at distances of 150-5500 meters ground-to-ground and 150-8000 meters air-to-ground. Activation of a shooter platform's laser rangefinder or interrogation button automatically triggers the BCIS interrogation, which sends an encrypted, directional query message to the targeted vehicle. If the targeted vehicle is friendly and equipped with BCIS, its transponder answers with an encrypted, omni-directional friend message. A friend light is illuminated in the shooter's sight, supplemented by voice confirmation. If no answer is received, a voice message indicates to the shooter that the target is unknown. The target identification process is completed in less than a second, enabling the shooter to make a rapid decision to engage or not.

Blue-Force Tracking (BFT) Systems

Blue-Force Tracking (BFT) systems seek to mitigate the risk of fratricide by supplying positional information regarding friendly units to enhance SA. An early attempt at such a system was the Radio Based Combat Identification (RBCI) device, which provided a software upgrade to combat Frequency Modulation (FM) radios to provide confirmation of the presence of RBCI-equipped friendly forces in hostile fire zones. The device could be used by troops acting as fire support coordinators, or by forward observers and air controllers conducting queries as part of their fires coordination and clearance procedures.

The Battlefield Target Identification Device (BTID) is an updated version of BCIS. However, whereas BCIS was strictly an IFF system, BTID provides a self-contained secure networking capability to support small-unit BFT applications. Like BCIS, BTID uses advanced mmW technology to query vehicles and receive friend-vs-foe data. BTID goes beyond BCIS by sharing data through the vehicle's onboard weapons system, allowing other operators to make engagement decisions instantly using shared real time identification data.

In 2002, the US Army fielded a new BFT system on vehicles in Iraq during Operation Iraqi Freedom (OIF) [17]. The BFT system consisted of a computer, satellite antenna, and Global Positioning System (GPS) receiver. These systems formed a tiered architecture using ground, airborne, and over-the-horizon (OTH) relay to track friendly forces and collate their positions, which are then transmitted to friendly units. The system employs a notebook-size, rugged, 12-inch diagonal daylight-visible computer display, strapped on or bolted into vehicles, as an interface for operators. The system delivers a near real-time display of the positions of friendly units in relation to one another. Other tactical data can be overlaid to help users assess their positions with respect to landmarks, terrain, mission objectives, and possible enemy positions. At command centers, the BFT system provides not just static snapshots of battle flow, but a near real-time common operational picture, including blue-force data and overlaid tactical data.

Although the BFT system has so far been implemented only on vehicles, the US Army has been investigating ways to implement BFT for individual soldiers [18]. In particular, efforts

have been made to make use of the capabilities of Commander's Digital Assistants (CDAs)[3] with which soldiers can input positional information for themselves or others. CDAs come equipped with GPS, a transceiver, and an "anti-spoofing" module to prevent the enemy from disrupting, imitating, or making use of signals. The CDA acts as both a sensor providing positional information to a central network and as an SA tool, presenting positional information about friendly units via the CDA screen.

Comparing IFF and BFT Systems

IFF and BFT systems are attractive as decision support tools because they offer the promise of enhancing combat effectiveness and reducing fratricide. Beyond this general appeal, each type of system has its own advantages and disadvantages as decision support tools.

IFF helps a shooter make timely decisions for a "shoot, no-shoot" decision at increased ranges. Furthermore, IFF is not dependent on networked communications and can be used when communications are unavailable or when operating under radio silence. However, IFF generally requires direct line of sight between shooter and target, and terrain screening or masking as well as range are issues in determining the effectiveness of IFF. IFF is also adversely affected by environmental factors such as dust, humidity, etc. that disrupt signals. IFF requires that both a shooter and friendly target be equipped with functioning transponder/receiver units, and failure of either will cause the system to fail. More fundamentally, from a decision making standpoint, negative feedback from an IFF is ambiguous as the target may be an enemy or a neutral party, or a friend without a functioning transponder. Thus, there is the potential for negative feedback to be misinterpreted.

BFT directly enhances SA by providing location information regarding friendly units. The benefit of BFT depends on the proportion of friendly units for which timely and accurate position information can be obtained. BFT also enhances joint/coalition interoperability through networking of blue-force positional data. Another advantage of BFT systems is that friendly position data can be fused with tactical data to further enhance SA. Finally, BFT systems that make use of GPS technology are very cost effective and highly accurate [17]. A significant weakness of BFT is that it depends on a sensor/communication network to gather data and to transmit an integrated picture. Such networks, unfortunately, are subject to failures that could leave units without access to BFT information. And like IFF, such networks can be affected by environmental factors. The effectiveness of a BFT system likely depends on its update frequency; if data are not updated regularly it loses value or becomes of negative value because assets can move quickly (the longer the delay, the less reliable is the picture). Although the goal for a BFT system is real-time position data, in practice this is extremely difficult to achieve and such systems typically suffer a lag of several minutes [19]. This may be too long to maintain an accurate picture when units are on the move, especially at high speed.

---

[3] The CDA is similar to commercially available PDAs (Personal Digital Assistants).

Overview of Experiments

Although BFT and IFF systems are being evaluated by Canada and its coalition partners, this evaluation has focused on the technical aspects of the systems rather than their impact on SA and effective decision making. The purpose of the two experiments reported here was to examine the effectiveness of IFF and BFT decision support for dismounted infantry soldiers. In light of the cost and effort involved in developing a CID system for dismounted soldiers, it is important to determine whether or not both types of systems can provide benefits to soldiers' combat effectiveness and reduce fratricide. In addition, the experiments examined the impact of conditions that might reduce the effectiveness of such systems.

To make an assessment of these two systems, we need an environment in which we can systematically assess the impact of system on human decision maker. The two experiments were conducted using the *IMMERSIVE* (Instrumented Military Modeling Engine for Research using SImulation and Virtual Environments) software platform developed at Defence Research and Development – Canada (DRDC) Valcartier. The IMMERSIVE platform is based on a modified gaming environment called "Unreal Tournament 2004," co-developed by commercial software companies Epic Games and Digital Extremes, that creates a first-person perspective environment in which the participant assumes the role of a dismounted infantry soldier. This platform was used to present subjects with blocks of trials in which each trial comprised a human figure moving into view. The subject's task was to engage (i.e., shoot) only those figures that were enemies. Friendly and enemy forces were distinguishable by differences in uniforms and equipment. Subjects remained at a specific fixed location in the simulated environment while targets entered into their field of view. The IMMERSIVE platform is a low-fidelity simulator but the environments and targets used in the experiments were developed with the support of people knowledgeable of Canadian Forces (CF) doctrine and procedures.

The first experiment directly compares CID performance when subjects have access to a rifle-mounted IFF or hand-held BFT system as opposed to no decision support whatsoever. The results of this experiment will set a benchmark for considering the potential benefits of such decision support systems (DSSs) for the dismounted infantry soldier.

In the case of a BFT system, the potential exists for delays in the updating of positional information regarding friendly units, which would reduce the value of the BFT. Existing BFT systems depend on a communications network that can freely share data among multiple platforms. Whether communications is done via radio, mmW, infrared, or laser signals, there exists the potential for signals to be disrupted by environmental conditions [20], equipment failure, or interference by outside sources, including deliberate disruption by the enemy [21]. Thus, it is important to know how the CID judgments made by human operators will be affected by disruption or delays in updating BFT information. Although IFF systems can potentially fail to provide accurate feedback, they are, unlike BFT, not subject to delays due to their design (i.e., direct, line-of-sight interrogation of targets). Experiment 2 investigates the impact of updating delays of a simulated handheld BFT device for dismounted infantry.

Experiment 1

Method

Subjects

Subjects were 24 male and female volunteers who were employees of DRDC Toronto, students conducting research at DRDC Toronto, or individuals recruited from local universities. All subjects were aged 18 and older, had normal or corrected-to-normal vision, and were unfamiliar with the specific hypotheses and stimulus configurations of the experiments. All received stress pay remuneration for participating.

This study, approved by the DRDC Toronto Human Research Ethics Committee (HREC), was conducted in conformity with the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans.

Materials and Procedure

The experiment was conducted with Personal Computers (PCs), which presented stimuli, collected subject responses, and recorded data. The IMMERSIVE platform was used as a test bed simulating combat activities. Subjects used the computer mouse to control the direction of facing and firing the weapon (by clicking the left mouse button).

The experimentation process comprised the set up, deployment, and management of the following experimentation components:

- Terrain: The simulated environment in which a scenario takes place;

- Scenario: A sequence of events representing a portion of battlefield action;

- roBOTic computer controlled entities (BOTs): Play scenario characters (see Figure 1);

- Participant: Plays the role of a Canadian soldier and controls a rifle that can be used to engage (shoot at) hostile entities; and

- ROE: Rules that govern how the participant responds to different kinds of BOTs.

Subjects were provided with ROE at the beginning of the experimental session. The ROE distinguished friendly from potentially hostile BOTs according to four characteristics of the soldier: 1) the weapon carried, 2) the uniform worn, 3) the type of walk (crouched or upright), and 4) whether or not the soldier had his/her rifle aimed. To establish a mission context, subjects were informed:

> *"In this experiment, you are manning a critical checkpoint. Recent intelligence has indicated that enemy combatants are planning to attack a local orphanage in order to spark conflicts among various ethnic and political factions. It is crucial that they not be allowed to succeed. It is only by taking out enemy combatants who pass your*

checkpoint that we will be able to prevent the planned atrocity. As you monitor your area of operation, keep in mind the criticality of stopping all enemies as quickly as possible."
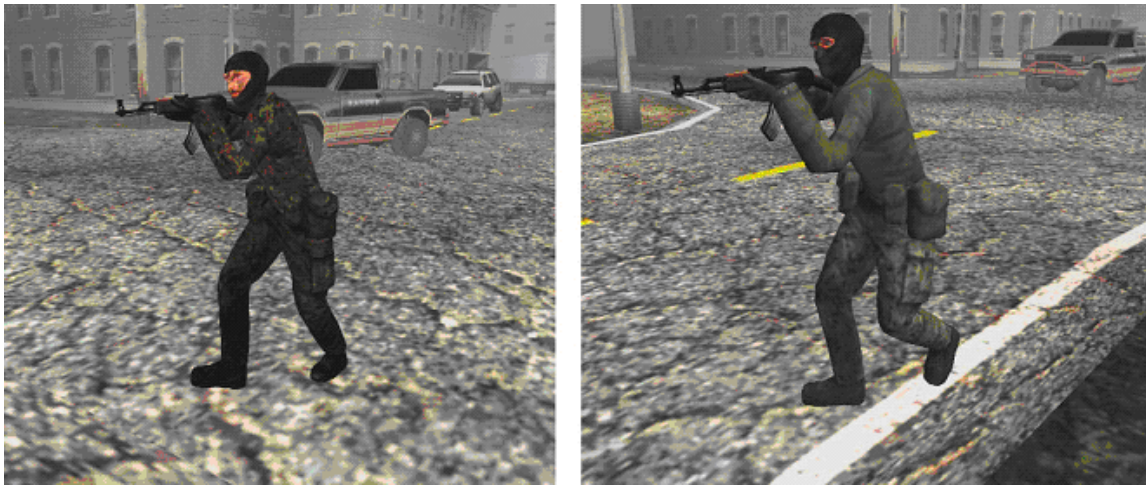

Figure 1. Examples of BOTs to be used in scenarios (pictures presented here are not as sharp as actual computer images).

Subjects in previous pilot studies had expressed a great deal of concern with avoiding incidents of fratricide and were thus overly cautious. The urgency of engaging enemies was emphasized in the instructions to ensure that subjects concentrated on both engaging enemies as well as avoiding fratricide.

Subjects performed three blocks of trials as a dismounted infantry soldier manning a fixed location. In Figure 2, the subject's location is marked by a white box at the bottom. In a block, a number of BOTs were in motion, following pre-specified paths at pre-specified times. Two such paths are marked in blue and red in Figure 2. The BOTs traveled into and out of view sequentially, so that no two BOTs were visible to the subject at the same time.

To control for effects of position and path of movement, a friendly and enemy BOT started at the same position and followed the same path on different trials in each block. Thus, subjects encountered a friend and enemy following the same path under the same conditions. The orders in which BOTs moved through the environment followed one of two orders (forward and reverse).

The IMMERSIVE software logged subject actions pertinent to subjects' firing decisions. The software logged each instance in which the subject fired the rifle, the identity of the BOT fired upon, and the subject's accuracy (whether or not the shot hit the BOT). The primary experimental measure was decision accuracy (i.e., whether or not the subject engaged a hostile or friendly BOT). A subject could fire one or more shots at a BOT without hitting it. To capture such events as intended engagements, the software logged for each shot fired whether it hit a BOT and, if not, how close the shot was to a BOT (i.e., minimal distance

between shot and BOT). Shots fired within a certain distance of a BOT (approximately one meter in the simulated environment) were counted as engagements.[4]
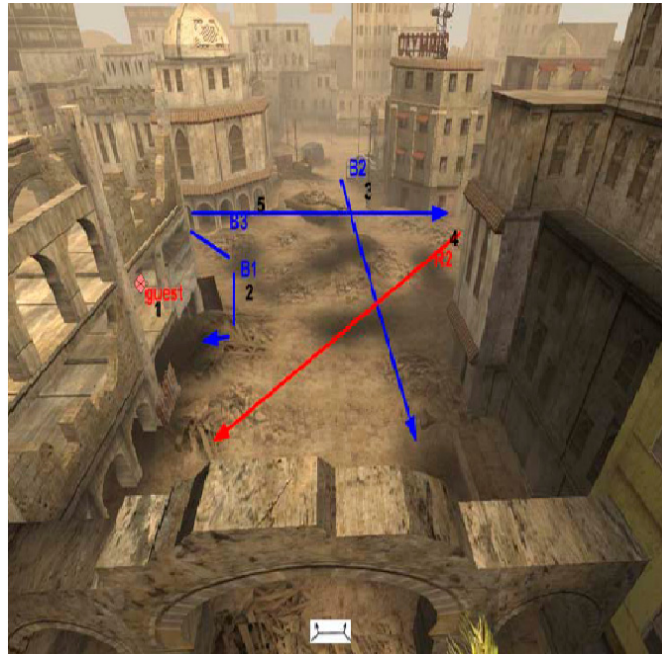

Figure 2. Example BOT paths in a simulated environment.

Response times were not considered because it was impossible to distinguish the target detection and target identification aspects of the task. Subjects did not provide any observable indication that they had detected a target. Thus, overall response times measured from the first appearance of a target would contain varying amounts of time reflective of the presence but not detection of that target, making response times unreliable across targets.

In the No DSS condition, subjects performed the task without access to any decision aid. In the Rifle IFF condition, subjects' rifles were equipped with a box containing a light. Subjects were instructed that when a target was in the rifle sight, they could press a marked key on the keyboard which would interrogate the target. If the target was a friend, the light would turn blue, as illustrated in the left panel of Figure 3. If the target was not a friend, the light would remain dark, as in the right panel of Figure 3. Although subjects were not forced to use the IFF when targeting, all subjects nevertheless did make full use of the IFF.

In the BFT condition, subjects could call up a simulated BFT device as a decision aid (see Figure 4). The device, which was modeled on a Personal Digital Assistant (PDA), presented a top-down map of the local area. Superimposed on the map were blue dots representing the position of friendly soldiers. Subjects could call up the BFT device at any time during the experiment by pressing a specified key on the computer keyboard but were not required to use

---

[4] Because the criterion for engagement was a fixed distance with respect to a BOT, the angular displacement from rifle to BOT varied somewhat with the distance of the BOT to the subject's firing position. However, angular displacements were not computed for each shot because the range of firing angles associated with engagements was fairly small.

it. Implemented as a PDA, the BFT was intended to be viewed periodically to ascertain positions of friendly units.

Figure 3. Rifle-mounted IFF device used in Experiment 1, which blue light on to indicate friend and unlit to indicate not-a-friend.

Figure 4. Simulated BFT device available to subjects in Experiment 2

Design

The main factor varied within-subjects was the type of DSS available to the subject. All subjects completed three conditions for this factor: 1) a No DSS control condition in which subjects had no support, 2) a Rifle IFF condition in which subjects had a rifle-mounted IFF system, and 3) a BFT condition in which subjects could call up a BFT display whenever desired. The order in which subjects completed the three conditions was counterbalanced across all subjects.

Results

Subjects' decisions to shoot or to not shoot were recorded for each BOT in each DSS condition. Decisions to shoot an enemy BOT were termed *hits* and comprised correct recognition of an enemy, whereas decisions to not shoot an enemy BOT were termed *misses* and comprised failures to recognize an enemy leading to reduced mission effectiveness. Decisions to not shoot friendly BOTs were termed *correct rejections* and comprised the correct recognition of a friend, whereas decisions to shoot a friendly BOT were termed *false alarms* and comprised the incorrect determination of an enemy, leading to an instance of fratricide.

Subjects' use of the IFF and BFT was monitored in the respective conditions to ensure that subjects did actually use the devices. The IFF was consistently used when targeting BOTs. The BFT was regularly inspected by all subjects but the timings and durations of use were not recorded.

Hit Data

Figure 5 shows Hit rates calculated for each DSS condition. As can be seen, hit rates were fairly high in all conditions but larger in the Rifle IFF and BFT than No DSS condition. A single factor, within-subjects Analysis of Variance (ANOVA) indicated that DSS Condition had a significant effect on subjects' mean Hit rate [F(2,46) = 28.77, *Mean Square Error (MSe)* = 0.003, *p*<.05].

To better understand how Hit Rate varied across conditions, a series of post-hoc comparisons were performed using Fisher's Least Significant Difference (LSD) method, which computes an LSD value for each pair-wise comparison of means and determines the probability that the difference was the result of random chance. The results of the comparisons are summarized in Table 2.

Table 2. Fisher's Least Significant Difference (LSD) Test Results (Hit Rate)			
	No DSS	**Rifle IFF**	**BFT**
No DSS	N/A	*<.001*	*<.001*
Rifle IFF	-	N/A	0.614
BFT	-	-	N/A
Within MS_e = 0.033; *df* = 46 Contrasts which are significant to p<.05 are shown in **bold italic**			

The post-hoc contrasts confirm that the Hit Rate in the No DSS condition was significantly lower than that in both the Rifle IFF and BFT conditions. Hit rates in the latter two conditions, however, did not differ significantly from one another.

Figure 5. Hit rates (correct engagement of enemy) across DSS Condition.

False Alarm (FA) Data

Figure 6 shows FA rates calculated for each block. A single factor, within-subjects ANOVA revealed a significant effect of DSS Condition subjects' mean FA rate [$F_{(2,46)} = 7.83$, $MSe = 0.007$, $p < .05$]. To better understand how FA rate varied across conditions, a series of post-hoc comparisons was performed using Fisher's LSD method. The results of the comparisons are summarized in Table 3.

Table 3. Fisher's Least Significant Difference (LSD) Test Results (FA Rate)			
	No DSS	**Rifle IFF**	**BFT**
No DSS	N/A	*0.001*	*0.002*
Rifle IFF	-	N/A	0.724
BFT	-	-	N/A
Within MSe = 0.007; df = 46			
Contrasts which are significant to p<.05 are shown in **bold italic**			

The post-hoc contrasts show that the FA Rate in the No DSS condition was significantly greater than that in both the Rifle IFF and BFT conditions. The FA rates in the latter two conditions did not differ significantly from one another.
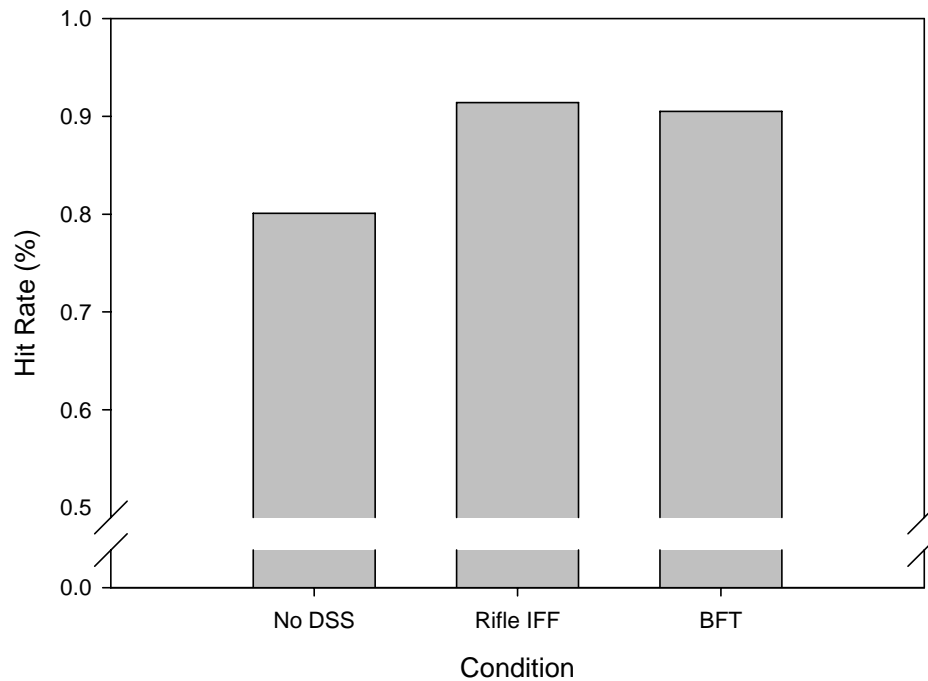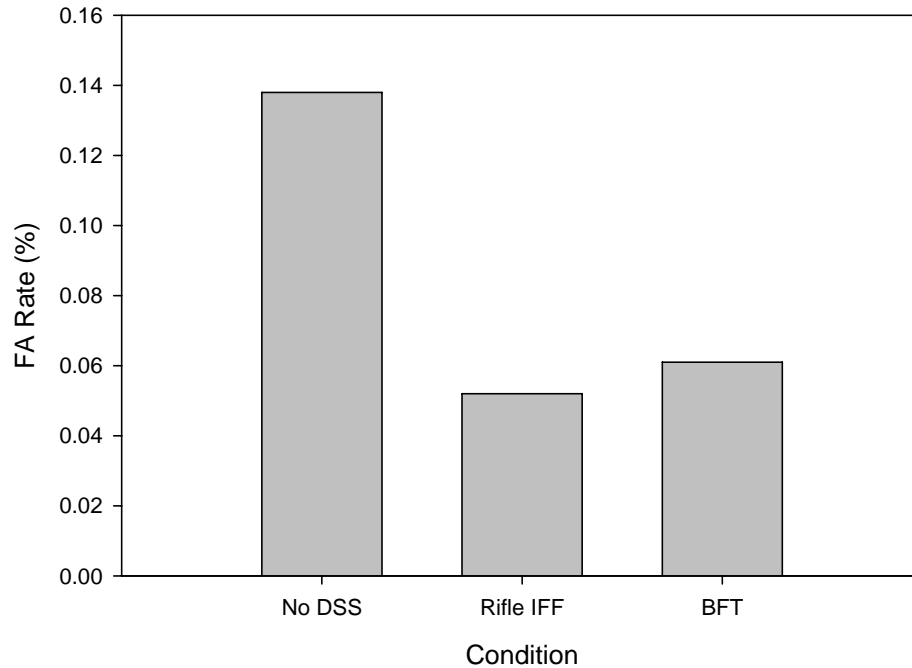

Figure 6. FA rates (incorrect engagement of friend) across BFT Condition

Sensitivity (*d'*)

Signal Detection Theory (SDT) [20] is a way to examine subjects' sensitivity to stimuli. In the context of the CID task, sensitivity refers to subjects' psychological discrimination between friends and foes, or their ability to correctly classify a friend as a friend and a foe as a foe. As a statistical measure, sensitivity (*d'*) is defined in terms of *z*, the inverse of the normal function and the observed hit and FA rates [21] by the formula:

$$d' = z(H) - z(FA) \tag{1}$$

Figure 7. Mean d' Values (Sensitivity) across all blocks of trials.

The z-transformation converts the hit and FA rates to standard deviation units such that a d' value of zero corresponds to a complete inability to distinguish friend from foe. Increasingly positive values of d' indicate progressively greater ability to discriminate friend from foe. Sensitivity takes into account correct engagements of enemy BOTs and correct non-engagements of friendly BOTs and is thus a more complete measure of performance than hit rate or FA rate alone.
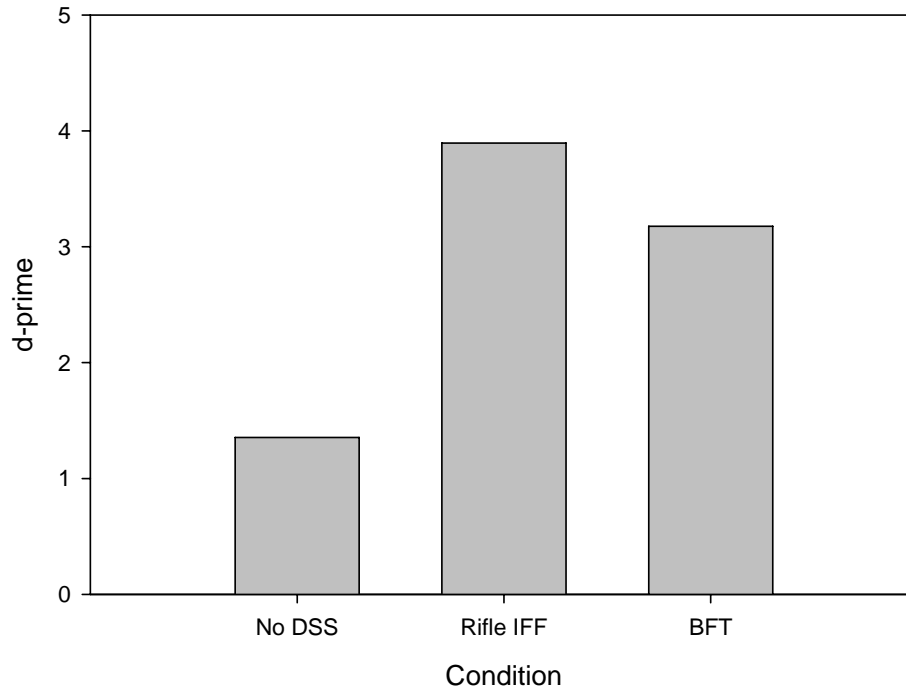
Figure 7 shows mean d' scores across DSS condition. A single factor, within-subjects ANOVA indicated that DSS Condition had a significant effect on subjects' mean d' scores [$F(2,46) = 17.470$, $MSe = 2.355$, $p<.05$]. To better understand how FA rate varied across conditions, a series of post-hoc comparisons was performed using Fisher's LSD method. The results of the comparisons are summarized in Table 4.

Table 4. Fisher's Least Significant Difference (LSD) Test Results (d')			
	No DSS	**Rifle IFF**	**BFT**
No DSS	N/A	***<0.001***	***<0.001***
Rifle IFF	-	N/A	0.113
BFT	-	-	N/A
Within MSe = 0.007; df = 46. Contrasts which are significant to p<.05 are shown in ***bold italic***			

The post-hoc contrasts show that mean d' was significantly greater in the Rifle IFF and BFT conditions compared to the No DSS condition. Although mean d' was somewhat larger in the Rifle IFF than BFT condition, this difference was not statistically significant.

Response Bias (*c*)

Derived from SDT, response bias is a measure of a subject's general tendency to respond positively to a target. In the case of the current experiment, it measures the general tendency to report a foe regardless of the actual identity of the target.
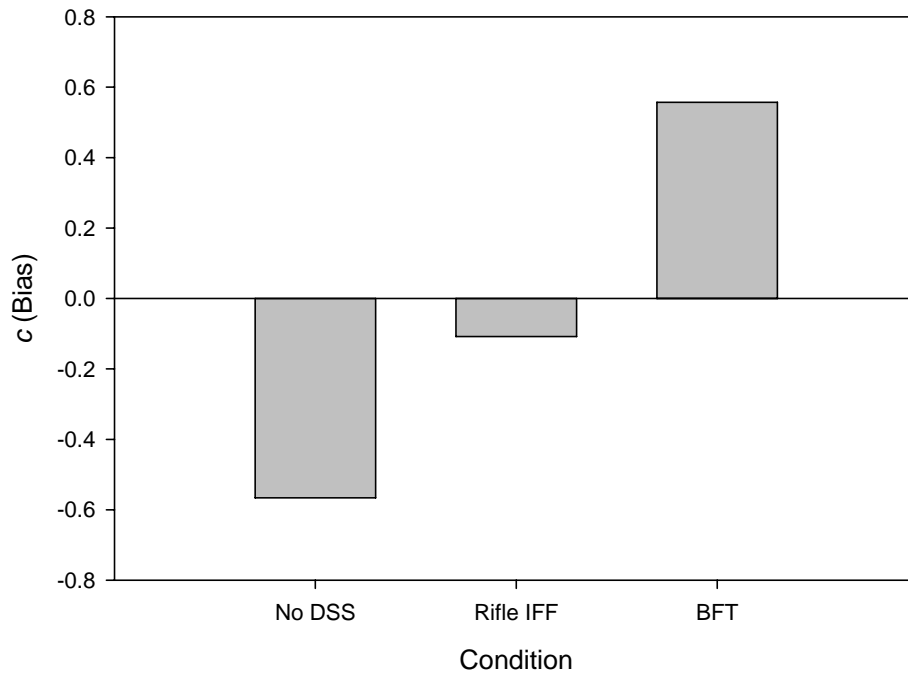
Figure 8. Mean c Values (Response Bias) across DSS Conditions.

Like sensitivity (d'), response bias (c) is defined in terms of z and the observed hit and FA rates [17]:

$$c = -0.5 \bullet [z(H) + z(FA)]$$
(2)

Positive values of c indicate a tendency to classify a target as foe regardless of its true identity, whereas negative values indicate a tendency to classify a target as a friend. The larger the value in either direction, the greater the tendency.

Mean c values are shown in Figure 8. Whereas subjects showed negative bias (i.e. a tendency to not engage) in the No DSS and Rifle IFF conditions, they exhibited positive bias (i.e. tendency to engage) in the BFT condition. To better understand how c values varied across conditions, a series of post-hoc comparisons was performed using Fisher's LSD method. The results of the comparisons are summarized in Table 5. All conditions differed significantly

from one another. Thus, it is clear that both Rifle IFF and BFT changed subjects' bias, reducing or even reversing a negative bias.

Table 5. Fisher's Least Significant Difference (LSD) Test Results (d')			
	No DSS	**Rifle IFF**	**BFT**
No DSS	N/A	*0.028*	*<0.001*
Rifle IFF	-	N/A	*0.002*
BFT	-	-	N/A
Within MSe = 0.002; df = 46.			
Contrasts which are significant to p<.05 are shown in **bold italic**			

Summary

Both the Rifle-mounted IFF and the BFT devices significantly increased Hit rates and decreased FA rates compared to the No DSS control condition. Similarly, subjects exhibited greater sensitivity (d') in the Rifle IFF and BFT conditions. These results clearly demonstrated that subjects performed better overall when they were able to use a DSS device than perform the task without assistance. The Rifle IFF and BFT conditions did not differ significantly in Hit rate, FA rate, or d'. Thus, these systems provided essentially the same benefit to performance.

The Rifle IFF and BFT conditions, however, did differ in mean c values. Whereas subjects exhibited essentially no response bias when using the rifle-mounted IFF, they exhibited some positive bias when using the BFT. This indicates that subjects had a general tendency to engage targets only when using the BFT. In contrast, subjects showed negative bias in the No DSS condition, indicating a general tendency to not engage targets.

Experiment 2

The goal of BFT systems is to provide instantaneous real-time data. However, it is not always possible to do this as existing BFT systems depend on a communications network that can be adversely affected by weather, terrain, and mechanical failure. When using a BFT system, some degree of lag in the updating of positional information can be realistically expected to occur. Delays between movement of friendly units and the updating of a hand-held BFT could seriously reduce the usefulness of such a device. Presumably, dismounted soldiers would require highly accurate information as they operate in relatively small areas. This experiment looked at the effect of a 10 second delay in the BFT device update on subjects' CID performance. The choice of a 10 second delay was somewhat arbitrary but this time interval has been identified as a target for timely updating of BFT systems in previous exercises (e.g., Bold Quest). For example, the BTID Digital Data Link (DDL), using a mmW waveform, provided position updates and refresh rates of less than 10 seconds, which was considered a timely SA capability between ground platforms to exchange friendly force tracking information. Systematic investigation of the impact of longer and shorter delays are anticipated.

Subjects completed four blocks of trials in which they encountered friendly and enemy units; a baseline with no BFT delay, a block with a 10 second delay where the participant is not informed of the delay, a block with an informed 10 second BFT delay, and a post-baseline with no BFT delay.

Method

Subjects

Subjects were 24 male and female volunteers who were employees of DRDC Toronto, students conducting research at DRDC Toronto, or individuals recruited from local universities. All subjects were aged 18 and older, had normal or corrected-to-normal vision, and were unfamiliar with the specific hypotheses and stimulus configurations of the experiments. All received stress pay remuneration for participating. Data of one subject was discarded due to overall low performance levels.

This study, approved by the DRDC HREC, was conducted in conformity with the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans.

Materials and Procedure

The experiment was conducted with the IMMERSIVE platform used in the previous experiment. As before, subjects were provided with ROE at the beginning of the experimental session that distinguished friendly from potentially hostile BOTs and governed when the subject is to engage hostile BOTs with the rifle.

Subjects performed four blocks of trials as a dismounted infantry soldier manning a fixed location. Subjects followed the same procedure as that of Experiment 1, including a practice

session prior to the experimental blocks in order to familiarize them with the IMMERSIVE platform and controls. As in Experiment 1, computer-controlled BOTs followed pre-specified paths at pre-specified times and traveled into and out of view sequentially, so that no two BOTs were visible to subjects at the same time.

In all blocks, subjects could call up a simulated BFT device as a decision aid (see Figure 4). As in Experiment 1, it presented a top-down map of the local area with blue dots representing the position of friendly soldiers. Subjects could call up the BFT device at any time during the experiment by pressing a specified key on the computer keyboard.

Design

The main condition of interest in this experiment was the BFT condition. Subjects performed the first block of trials with a BFT that provided real-time data on friendly BOTs' positions (BFT). The first BFT condition served to measure subjects' baseline performance with a BFT device that provided instantaneous, real-time data. Subjects then performed two blocks in which the position information provided by the BFT lagged by 10 seconds after events in the simulated environment (i.e., data shown by the BFT were 10 seconds old). In the first of these delayed conditions, subjects were not told that the data lag existed (10 second no warning), whereas in the following block subjects were told that BFT data lagged by 10 seconds (10 seconds warning). In the final block (End BFT), the BFT returned to real-time data.

To control for effects of position and path of movement, a friendly BOT and an enemy BOT started at the same position and followed the same path on different trials in each block. Thus, subjects encountered a friend and enemy following the same path under the same conditions. The orders in which BOTs moved through the environment followed one of two orders (forward and reverse).

Results

Subjects' decisions to shoot or to not shoot were recorded for each BOT in each BFT condition. *Hits*, *misses, correct rejections,* and *false alarms* were defined as in Experiment 1.

Hit Data

Figure 9 shows Hit rates calculated for each BFT condition. Overall, hit rates were relatively high, exceeding 90% in all blocks. A single factor, within-subjects ANOVA indicated that hit rate did not significantly vary across BFT condition [$F(3,63) = 2.60$, $MSe = 0.005$, *n.s.*]. The order in which BOTs appeared to subjects did not have a significant effect on hit rate [$F(1,21) = 1.20$, $MSe = 0.017$, *n.s.*], nor did this factor interact with trial block [$F(3,63) = 0.10$, $MSe = 0.005$, *n.s.*].

Figure 9. Hit rates (correct engagement of enemy) across BFT Condition.

False Alarm (FA) Data

Figure 10 shows FA rates calculated for each block. FA rates were dramatically lower in the first and end baseline conditions than in the two BFT conditions. A single factor, within-subjects ANOVA indicated that trial Block had a significant effect on subjects' mean FA rate [$F(3,63) = 9.89$, $MSe = 0.025$, $p < .01$]. The order of friendly and enemy BOTs did not have a significant effect on FA rate [$F(1,21) = 1.36$, $MSe = 0.063$, *n.s.*], nor did this factor interact with trial block [$F(3,63) = 2.07$, $MSe = 0.025$, *n.s.*].
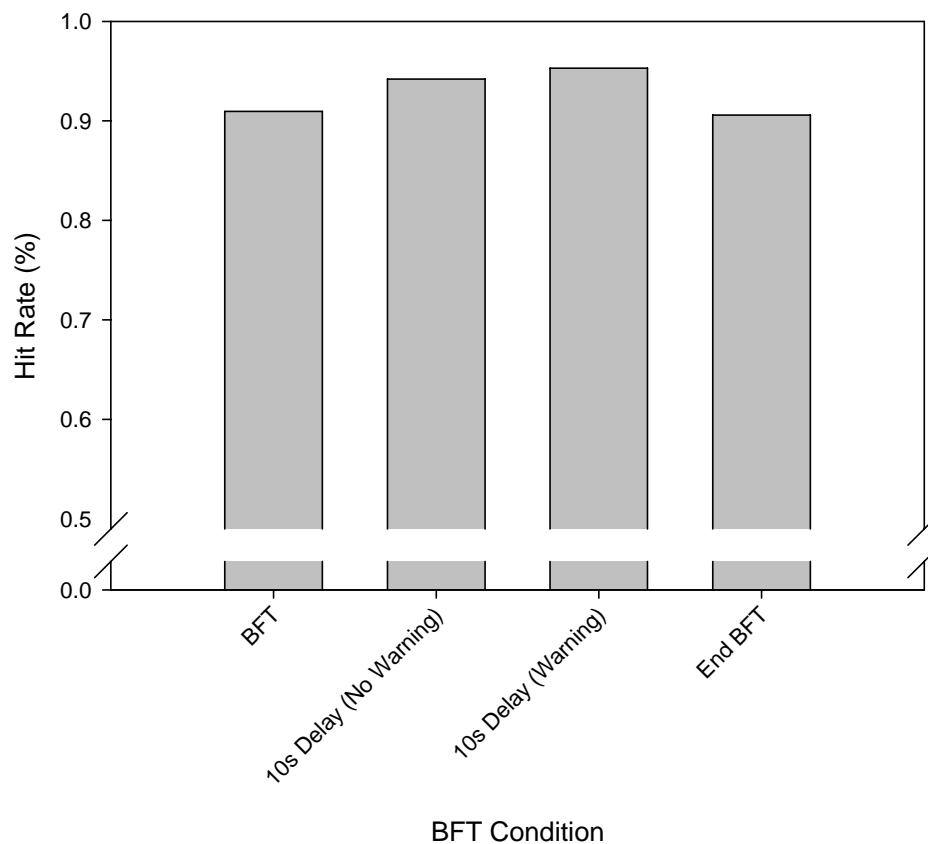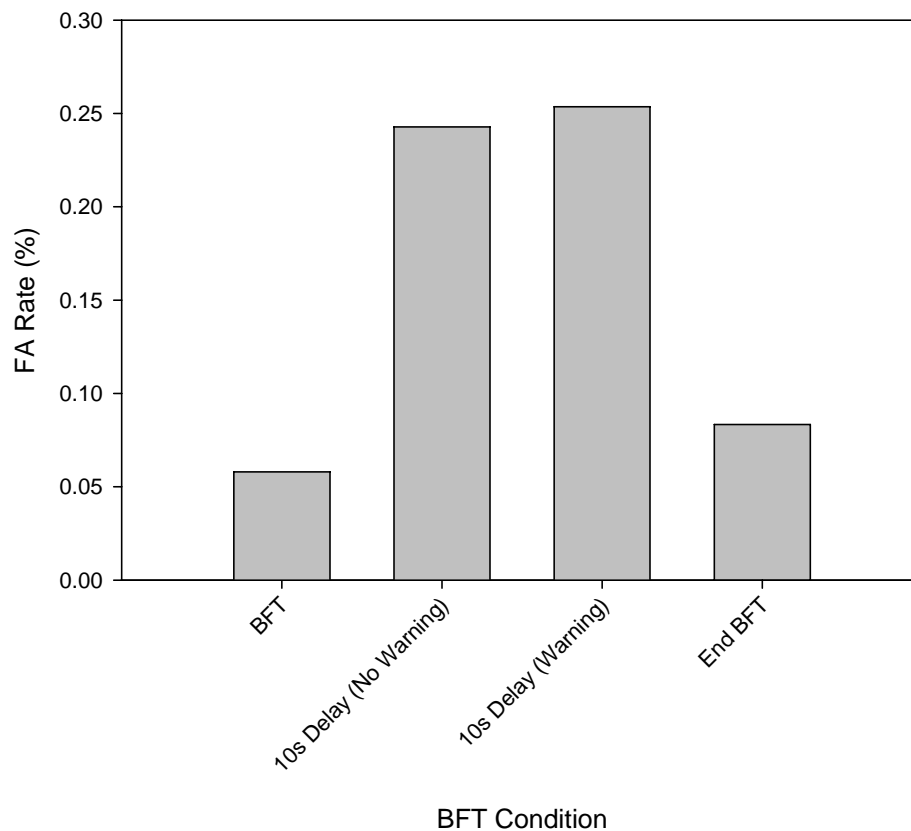
BFT Condition

Figure 10. FA rates (incorrect engagement of friend) across BFT Condition

To better understand how FA rate varied across blocks, a series of Fisher's LSD post-hoc comparisons (Table 6) was performed to contrast each block with every other block. .

		Table 6. Fisher's Least Significant Difference (LSD) Test Results (FA Rate)		
	BFT	**10s Delay (No Warning)**	**10s Delay (Warning)**	**End BFT**
BFT	N/A	*<0.001*	*<0.001*	0.599
10s Delay (No Warning)	-	N/A	0.822	*0.001*
10s Delay (Warning)	-	-	N/A	*<0.001*
End BFT	-	-	-	N/A
s indicates seconds Within *MSe* = 0.266; df = 66. Contrasts which are significant to p<.05 are shown in ***bold italic***				

The BFT and End BFT FA rates did not differ significantly, indicating no learning effect across the course of the experimental session. However, both the BFT and End BFT FA rates were significantly lower than those of the 10 second Delay (No Warning) and 10 second Delay (Warning) conditions. FA Rates in those two delay conditions did not differ from one another.

Sensitivity (*d'*)

The mean *d'* score for each subject was computed using the *z*-transformations of his or her Hit and FA rates, as described in Experiment 1.

Figure 11. Mean d' Values (Sensitivity) across all blocks of trials.

Figure 11 shows mean *d'* scores for each block. Sensitivity did not vary across BFT conditions [F(3,63) = 1.97, *MSe* = 1.808, *n.s.*]. The order in which BOTs appeared to subjects did not have a significant effect on hit rate [F(1,21) = 0.31, *MSe* = 4.647, *n.s.*], nor did this factor interact with trial block [F(3,63) = 0.34, *MSe* = 1.808, *n.s.*].
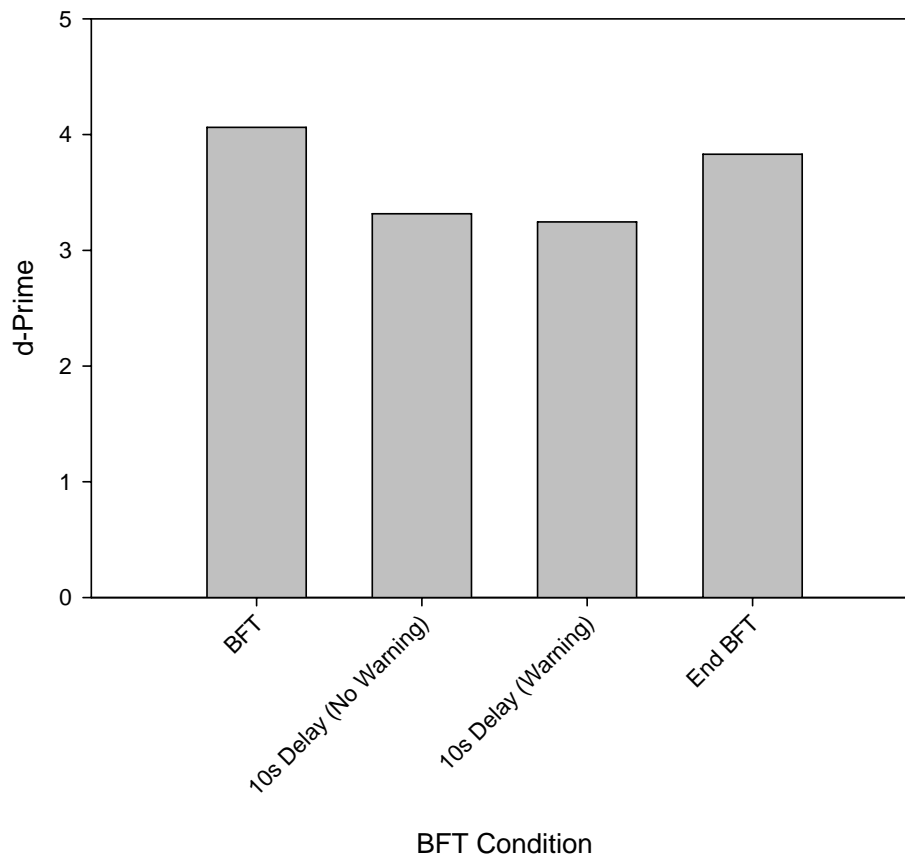
Response Bias (*c*)

The mean *c* score for each subject was computed by the method described in Experiment 1. Positive values of *c* indicate a tendency to classify a target as foe regardless of its true identity, whereas negative values indicate a tendency to classify a target as a friend. The larger the value in either direction, the greater the tendency.

Subjects exhibited small, negative *c* values in the BFT and End BFT conditions but much larger, positive values in the 10 second Warning and 10 second No Warning conditions. A single factor, within-subjects ANOVA indicated that BFT condition had a significant effect on subjects' mean *c* values [$F(3,63) = 8.65$, $MSe = 0.386$, $p < .01$]. The order of friendly and enemy BOTs did not have a significant effect on *c* values [$F(1,21) = 0.86$, $MSe = 1.172$, *n.s.*], nor did this factor interact with trial block [$F(3,63) = 1.99$, $MSe = 0.386$, *n.s.*].
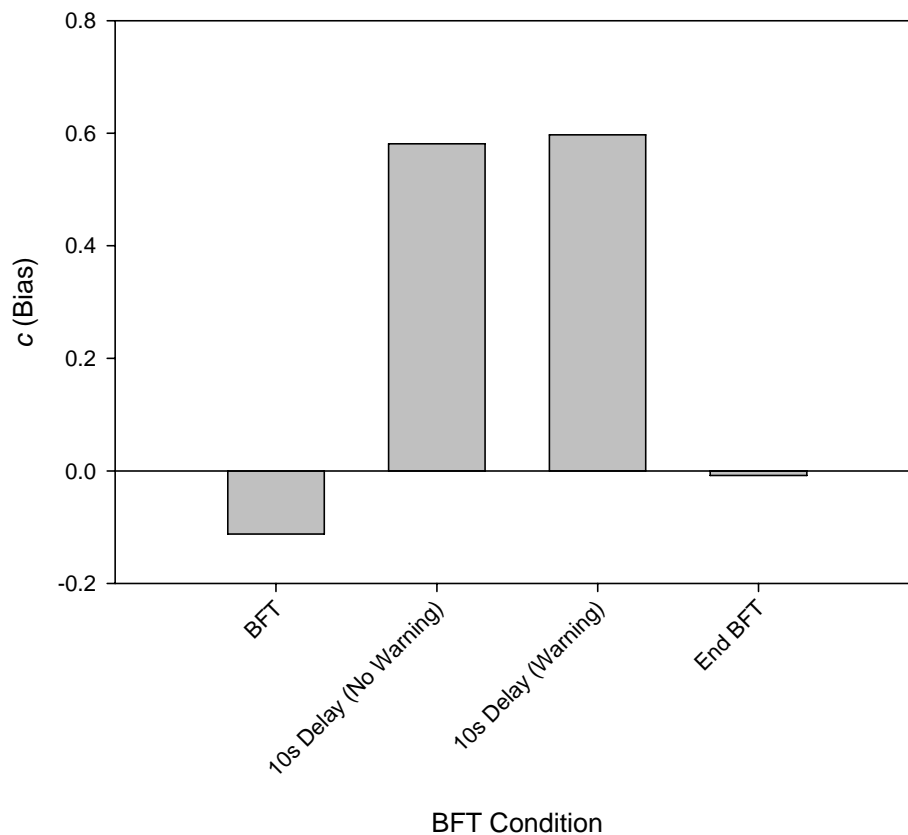
Figure 12. Mean c Values (Response Bias) across all blocks of trials.

To better understand how *c* values varied across conditions, a series of post-hoc comparisons was performed using Fisher's LSD method to contrast each block with every other block. The results of the comparisons are summarized in Table 7.

The BFT and End BFT *c* values did not differ significantly. However, c values in both the 10 second Delay (No Warning) and 10 second Delay (Warning) conditions

significantly exceeded those in the BFT and End BFT conditions. Thus, subjects who exhibited no bias, or slightly negative bias, when the BFT provided real-time data, exhibited a significant bias toward engaging a target when the BFT presented lagged data.

Table 7. Fisher's Least Significant Difference (LSD) Test Results (c)				
	BFT	**10s Delay (No Warning)**	**10s Delay (Warning)**	**End BFT**
BFT	N/A	***<0.001***	***<0.001***	0.580
10s Delay (No Warning)	-	N/A	0.933	***0.002***
10s Delay (Warning)	-	-	N/A	***0.002***
End BFT	-	-	-	N/A
s indicates seconds Within *MSe* = 0.266; df = 66. Contrasts which are significant to p<.05 are shown in **bold italic**				

It is interesting to note that subjects who used a real-time BFT in Experiment 1 exhibited positive bias, which was not replicated in this experiment. Response bias is likely governed by more factors than just the type of CID decision support available.

Summary

Adding a 10 second delay to the updating of position information in the BFT did not significantly impair subjects' ability to identify enemies. Both Hit rate and d' remained essentially the same in the two 10 second delay conditions as the real-time control condition. The 10 second delay did, however, significantly increase subjects' FA rate. This was true whether they were warned of the delay or not. In addition, subjects exhibited a strong response bias toward engaging targets in both 10 second delay conditions. Overall, a delay in BFT updating made subjects significantly more likely to engage friendly BOTs compared to real-time BFT data.

General Discussion

Fratricide is a prevalent threat on the battlefield. Various attempts to reduce the frequency of fratricide incidents have focused primarily on equipping vehicles with IFF or BFT devices. IFF devices assist the target identification process by providing indication when a shooter has targeted a friendly unit equipped with the appropriate transponder. BFT devices present positional information concerning friendly units to enhance SA.

IFF and BFT have different approaches to supporting CID. IFF supports target identification by providing a highly reliable signal when a shooter has targeted a friendly unit equipped with the appropriate transponder. The value of IFF is reduced in asymmetric conflicts where both hostile and neutral entities are in close proximity and negative feedback does not distinguish between them. In contrast, BFT does not directly support target identification but rather enhances global SA by providing location information of all friendly units. Although SA is important in anticipating where friends are going to be, the soldier must still make target identifications for each encountered entity. For this reason, BFT seems to be vulnerable to updating delays that result in an old picture being propagated and potentially leading to false beliefs about where friendly units are currently located.

Current technology does not yet exist to place these devices on individual dismounted soldiers but it is likely such technology will exist in the near future. Given that IFF and BFT remain viable candidates for decision support to CID, we investigated the potential impact of IFF and BFT devices for dismounted infantry soldiers in a simulated combat environment. The two experiments provide some insight into the potential benefit of IFF and BFT to CID decision making as well as the impact of system delays on the usefulness of BFT.

The first experiment directly compared CID performance when subjects had access to a rifle-mounted IFF or hand-held BFT system as opposed to no decision support whatsoever. It was found that both devices significantly reduced the frequency of false alarms (fratricide) while having no negative impact on hit rates (correct engagements of the enemy). In fact, subjects exhibited greater sensitivity when using the IFF and BFT devices. The rifle-mounted IFF and BFT devices did not differ in the extent to which they reduced FA rates compared to the control condition but subjects exhibited little or no response bias when using the IFF device. In contrast, subjects exhibited a positive response bias with the BFT, indicating a general tendency to engage potential targets.

The second experiment examined the impact of a 10 second delay or lag in updating of positional information on subjects CID performance. Although the delay did not reduce Hit rate or sensitivity compared to performance with a BFT providing instantaneous real-time data, it did result in significantly greater FA rate. This was true when subjects had not been warned of the updating lag but also when they were told about it. Thus, even when subjects knew the BFT was providing data that were not current, they were significantly more likely to engage friends than in the control condition. Subjects also exhibited a response bias to engage all targets when the BFT data lagged as opposed to essentially no bias when the data were real-time.

Taken together, the results of the experiments indicate the promise of personal IFF and BFT devices to drastically reduce the likelihood of fratricide by dismounted infantry soldiers on other soldiers. The results, however, also indicate that the effectiveness of these devices can

be dramatically reduced or even abolished when the devices do not work perfectly in real time. Given normal operational conditions that include inclement weather, dust and other environmental factors that can disrupt the functioning of IFF and BFT devices, it is crucial to further examine how the decision making of the human user of these devices will be affected by factors that reduce their effectiveness.

It will be important in future research to conduct evaluations in real-world settings as well as simulation platforms. Although the IMMERSIVE platform used here presents an engaging and challenging CID task, it is a low fidelity simulation. It uses low resolution graphics and, more importantly, dramatically simplifies the task and environmental conditions under which a soldier operates. The main advantage of the IMMERSIVE platform is the high degree of experimental control it allows. Thus, initial studies using the IMMERSIVE platform can provide indications of the potential benefits and weaknesses of CID support systems but further validation is needed to confirm that these benefits and weaknesses extend to operational settings. It is likely that many of the effects observed in a simulation environment will be attenuated or otherwise affected by the kinds if operational factors (weather, stress, etc.) that cannot be easily simulated in the laboratory.

References

1. Defense Science Board (1996). *Defense Science Board Task Force on Combat Identification*. Report Number: 20301-3140.

2. Dean, D. F., & Handley, A. (2006). *Representing the human decision maker in combat identification*. Proceedings of the 2006 Command and Control Research and Technology Symposium.

3. Dean, D., Vincent, A., Mistry, B., Hynd,K. and Syms P.R.(2005) *The Integrative Combat Identification Entity Relationship (INCIDER) conceptual model*. Technical Working Paper. Fareham, Hants. Ministry of Defence.

4. Karsh, R., Walrath, J. D., Swoboda, J. C., & Pillalamarri, K. (1995). *Effect of battlefield combat identification system information on target identification time and errors in a simulated tank engagement task.* (Technical report ARL-TR-854). Aberdeen Proving Ground, MD, United States: Army Research Lab.

5. Harris, M.J. and Syms, P.R. (2002). *Land fratricide and IFF OA review*. Farnborough, Hampshire, Defence Science and Technology Laboratory UK.

6. US Congress, Office of Technology Assessment (1993). *Who goes there: Friend or foe?* Office of Technology Assessment Report (OTA-ISC-537). U.S. Government Printing Office: Washington, DC.

7. Cruz, E. E. (1996). *Fratricide in air-land operations*. Unpublished Master's thesis. Naval Postgraduate School, Monterey, CA.

8. Allegretti, B.P. (2000). *Situational awareness data requirements for a combat identification network.* Master's Thesis. Naval Postgraduate School.

9. Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review, 63*, 81-97.

10. Kogler, T. M. (2003). *The effects of degraded vision and automatic combat identification reliability on infantry friendly fire engagements*. Army Research Laboratory (ARL-RP-0065). Aberdeen Proving Ground, MD.

11. Doton, L. (1996). Integrating technology to reduce fratricide. *Acquisition Review Quarterly, Winter*, 1-18.

12. Shuck, T. M., Hunter, J. B., & Wilson, D. D. (2004). *Multi-hypothesis structures, taxonomies, and recognition of tactical elements for combat identification fusion*. Proceedings of the 9th International Command and Control Research and Technology Symposium, Copenhagen, Denmark.

13. Hart, R. G. (2007). Combat identification: It's all about combat effectiveness. *The Canadian Army Journal, 10*, 6-11.

14. Hayhurst, G. (1991). The case for IFF provision for UK ground forces. *Defense & Security Analysis*. http://www.informaworld.com/smpp/title~content=t713412200.

15. Rasmussen, R. E. (2007). *The wrong target: The problem of mistargeting resulting in fratricide and civilian casualties.* Unpublished Masters Thesis. Joint Advanced Warfighting School. Norfolk, VA.

16. Starr, B. (1993). U.S. advances on battlefield ID. *International Defense Review, December 26*, 961.

17. Rider, T. L. (2004). Blue force tracking to expand across force. *Army AL&T, September-October*, 2-5.

18. Ackerman, R. K. (2005). Army Intelligence Digitizes Situation Awareness. *Signal, July*.

19. Boyd, C.S., Collyer, R.S., Skinner, D.J., Smeaton, A.E., Wilson, S.A., Krause, D.W., Dexter, R.M., Perry, A.R., & Godfrey, J. (2005). Characterisation of combat identification technologies. *Proceedings of TENCON 2005 – 2005 IEEE Region 10 Conference*.

20. Green, D. M., & Swets, J. A. (1966). *Signal detection theory and psychophysics*. New York: Wiley.

21. Macmillan, N. A., & Creelman, C. D. (1991). *Detection theory: A user's guide*. Cambridge, UK: Cambridge University Press.

List of symbols/abbreviations/acronyms/initialisms

ACTD	Advanced Concept Technology Demonstrations
AFID	Anti-Fratricide Identification Device
ANOVA	Analysis of Variance
BCIS	Battlefield Combat Identification System
BFT	Blue-Force Tracking
BOTs	roBOTic computer controlled entities
BTID	Battlefield Target Identification Device
c	Response bias
C2	Command and Control
CCID	Coalition Combat Identification
CDAs	Commander's Digital Assistants
CF	Canadian Forces
CID	Combat Identification
d'	Response sensitivity
DDL	Digital Data Link
DRDC	Defence Research & Development Canada
DSS	Decision Support System
ESM	Electronic Support Measure
FA	False Alarm
FM	Frequency Modulation
GPS	Global Positioning Satellite
HREC	Human Research Ethics Committee
IFF	Identify-Friend-or-Foe
IMMERSIVE	Instrumented Military Modeling Engine for Research using SImulation and Virtual Environments
LSD	Least Significant Difference
mmW	Millimeter Wave
MSe	Mean Square Error
NATO	North Atlantic Treaty Organization
OIF	Operation Iraqi Freedom
OTH	Over-the-horizon
PC	Personal Computer
PDA	Personal Digital Assistant
RBCI	Radio Based Combat Identification

RF	Radio Frequency
ROE	Rules of Engagement
s	Seconds
SA	Situation Awareness
SDT	Signal Detection Theory
SOP	Standard Operating Procedures
TTPs	Tactics, Techniques, and Procedures
US	United States
USJFCOM	U.S. Joint Force Command

Distribution list

Document No.: DRDC TR 2009-214

LIST PART 1: Internal Distribution by Centre

2
2   TOTAL LIST PART 1

LIST PART 2: External Distribution by DRDKIM

1   Library and Archives Canada

DJCP
1   LCol Rick Johnston (Richard.Johnston@forces.gc.ca)
1   Cdr Robert Edwards (Robert.Edwards2@forces.gc.ca)

DRDC Valcatier
1   Dr. Eloi Bossé (Eloi.Bosse@drdc-rddc.gc.ca)

DST C4ISR 4
1   Dr. Benny Wong (Benny.Wong@forces.gc.ca)

CTC
1   Col Steve Bowes (Steve.Bowes@forces.gc.ca)
1   Maj Michael Standish (Michael.Standish@forces.gc.ca)

DGLS/COS Land Ops
1   Shawn Hoag (Shawn.Hoag@forces.gc.ca)

SJS
1   LCol Alan Smith (Alan.Smith@forces.cgc.ca)
1   Maj John Whalen (John.Whalen2@forces.gc.ca)

ADM(S&T)
1   LCol Peter Scott (Peter.Scott@forces.gc.ca)

DSTA
1   Luc Lefebvre (Luc.Lefebvre@forces.gc.ca)

DRDC Atlantic
1   Dr. Mark Gammon (Mark.Gammon@forces.gc.ca)

13   TOTAL LIST PART 2

15   TOTAL COPIES REQUIRED

DOCUMENT CONTROL DATA	
(Security classification of the title, body of abstract and indexing annotation must be entered when the overall document is classified)	

1. ORIGINATOR (The name and address of the organization preparing the document, Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's document, or tasking agency, are entered in section 8.) Publishing: DRDC Toronto Performing: DRDC Toronto Monitoring: Contracting:	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.) UNCLASSIFIED

3. TITLE (The complete document title as indicated on the title page. Its classification is indicated by the appropriate abbreviation (S, C, R, or U) in parenthesis at the end of the title) Comparison of Identify–Friend–Foe and Blue–Force Tracking Decision Support for Combat Identification (U) (U)

4. AUTHORS (First name, middle initial and last name. If military, show rank, e.g. Maj. John E. Doe.) David J. Bryant; David G. Smith

5. DATE OF PUBLICATION (Month and year of publication of document.) December 2009	6a NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 41	6b. NO. OF REFS (Total cited in document.) 21

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of document, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.) Technical Report Combat identification, decision making, blue force tracking, IFF

8. SPONSORING ACTIVITY (The names of the department project office or laboratory sponsoring the research and development – include address.) Sponsoring: Tasking:

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant under which the document was written. Please specify whether project or grant.) 5au	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document) DRDC Toronto TR 2009–214	10b. OTHER DOCUMENT NO(s). (Any other numbers under which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on the dissemination of the document, other than those imposed by security classification.) Unlimited distribution

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11), However, when further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.)) Unlimited announcement

DOCUMENT CONTROL DATA
(Security classification of the title, body of abstract and indexing annotation must be entered when the overall document is classified)

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

(U) Technologies to support Combat Identification (CID) are rapidly evolving and may be deployable to dismounted soldiers in the future. Two experiments examined the effectiveness of Identify–Friend–Foe (IFF) and Blue–Force Tracking (BFT) decision support for dismounted infantry soldiers. Subjects played the role of a dismounted infantry soldier in a first–person perspective environment and engaged a series of simulated targets. Subjects attempted to engage (i.e., shoot) only those figures that were enemies. Results demonstrated that subjects performed better overall when they were able to use a Decision Support System (DSS) than perform the task without assistance. There was no difference in effectiveness of the IFF and BFT systems. Adding a 10 second delay to the updating of position information in the BFT dramatically reduced the effectiveness of a BFT, regardless of whether subjects knew about the delay or not.

(U) Les technologies servant à appuyer l'identification au combat (IDCbt) évoluent rapidement et pourraient éventuellement être mises à la disposition de chaque soldat à pied. Deux expériences ont permis d'examiner l'efficacité des systèmes d'aide à la décision Identification ami ou ennemi (IAE) et Suivi des forces bleues (SFB) pour les fantassins à pied. Chacun des participants a joué le rôle d'un fantassin à pied dans une perspective de premier intervenant et devait engager une série de cibles simulées. Les sujets ne devaient tirer que sur les figures ennemies. Selon les résultats obtenus, les participants ont obtenu un meilleur rendement général lorsqu'ils ont eu recours à un système d'aide à la décision (SAD) que lorsqu'ils ont exécuté la tâche sans aide. Aucune différence n'a été notée quant à l'efficacité des systèmes IAE et SFB. Une période d'attente de 10 secondes appliquée à la mise à jour des données sur la position dans le système SFB a réduit sensiblement l'efficacité du SFB, sans égard au fait que les sujets étaient mis au courant du délai ou non.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

(U) combat identification, blue–force tracking, IFF

Defence R&D Canada

Canada's Leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

DEFENCE **R&D** DÉFENSE

www.drdc-rddc.gc.ca